Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method for communicating real-time to subscribers of an Internet Service Provider (ISP), comprising the steps of:

   a.   Accessing, by a redirecting device, only subscriber upstream traffic to a destination site requested by the subscriber, wherein the redirecting device inter-connects to Ethernet ports of a cable access concentrator;

   b.   Identifying, by the redirecting device, the subscriber to provide a unique subscriber identification based on the accessed subscriber upstream traffic automatically provided by the subscriber during communications via the cable access concentrator;

   c.   Providing, by the redirecting device, the unique subscriber identification to a consolidating and management device, wherein the consolidating and management device is separate from the redirecting device;

   d.   Determining, by the consolidating and management device, the subscriber associated with the unique subscriber identification, and, if a ~~bulletin~~ message for the subscriber is desired:[,]

      sending policy information to the redirecting device, wherein the policy information includes ~~at least one of: time of delivery, frequency, triggering activity, an associated web page to be delivered or other content to be delivered~~ an IP address the subscriber's device, and a message or a modification to be performed for the IP address;

      examining, by the redirecting device, the accessed upstream traffic to

2

determine if it is possible to send a redirection, ~~wherein the examining occurs without modifying the accessed upstream traffic~~; and

forcing a delivery of specially-composed messages according to policies set by the ISP irrespective of the subscriber's intended destination;

c.   If the ~~bulletin~~ message for the subscriber is not desired when no policy is in force for the subscriber, allowing, by the redirecting device, a direct connection from the subscriber to the destination site to proceed normally, ~~and sending, only by the destination site, downstream web traffic to the subscriber without forwarding the downstream web traffic by the redirecting device~~ without a proxy server or other device requiring access to downstream traffic;

f.   ~~If the bulletin message for the subscriber is desired, examining, by the redirecting device, the accessed upstream traffic to determine if it is possible to send a redirection, wherein the examining occurs without modifying the accessed upstream traffic; and~~

f[g].   Based on the policy information, sending to the subscriber by the redirecting device, the redirection for a different destination site.

2.   (previously presented) The method of claim 1, wherein the bulletin message is an area within a window on the subscriber PC's browser.

3.   (previously presented) The method of claim 1, wherein the bulletin message is a prompt provided on the subscriber PC.

4.   (previously presented) The method of claim 1, wherein the subscriber is a

3

customer identification comprising at least one of an account number, modem MAC address or serial number, or other fixed identifier.

5.   (cancelled)

6.   (previously presented) The method of claim 1, wherein the subscriber is identified to belong to a defined group of subscribers and wherein the bulletin message is selectively sent to a pre-selected subscriber group.

7.   (previously presented) The method of claim 1, wherein the examining step further includes working through Web browsers irrespective of the World Wide Web destination sought by the subscriber.

8.   (previously presented) The method of claim 7, further including the step of returning the subscriber to the original World Wide Web destination after the bulletin message has been transmitted.

9.   (previously presented) The method of claim 1, wherein the examining step is further adapted for working with multiple types of content.

10.   (previously presented) The method of claim 1, wherein the examining step is performed by a hardware device that can be simply connected at various points, in

4

plurality, in a provider infrastructure.

11. (previously presented) The method of claim 10, further including a plurality of said hardware devices.

12. (previously presented) The method of claim 10, further including the step of providing optional fail-safe operation of each device such that failure does not disrupt other normal browsing and Internet activity of the subscriber but results only in an interruption of bulletin message delivery.

13. (previously presented) The method of claim 1, wherein the examining step is provided by a software system installed on a computer system that is connected at various points, singly or in plurality, in a provider infrastructure.

14. (previously presented) The method of claim 13, further including a plurality of hardware devices, each including one of said software system.

15. (previously presented) The method of claim 13, further including the step of providing optional fail-safe operation of each device such that failure does not disrupt other normal browsing and Internet activity of the subscriber but results only in an interruption of bulletin message delivery.

16. (previously presented) The method of claim 1, further including the step of

5

defining a specific policy for controlling selective transmission of bulletin messages to the subscriber.

17.   (previously presented) The method of claim 16, further including the step of defining a policy that includes a Web URL or other page information.

18.   (original) The method of claim 16, further including the step of defining a policy that includes timing and frequency of delivery.

19.   (previously presented) The method of claim 16, further including the step of defining a policy for activating the redirecting device to deliver a message in response to a selected subscriber activity.

20.   (original) The method of claim 19, wherein the activity comprises a defined destination.

21.   (previously presented) The method of claim 19, wherein the activity comprises an amount of activity by the subscriber.

22.   (previously presented) The method of claim 19, wherein the activity comprises a request carrying a signature of virus contamination.

6

23.   (original) The method of claim 1, further including the step of generating a plurality of independently designated policies to be delivered correctly to the subscriber even if some policy events invoke in simultaneity.

24.   (previously presented) The method of claim 23, wherein the examining step includes an ability to acquire knowledge of the policies and the identifier when a Web or other request is detected with only an identifying IP address.

25.   (previously presented) The method of claim 24, wherein the examining step is further adapted for minimizing overhead of acquiring subscriber parameters through caching of subscriber information for a determined portion of time.

26.   (previously presented) The method of claim 1, wherein the examining step is further adapted for use in connection with the consolidating and management device for permitting a group of redirecting devices to be viewed as a single system.

27.   (previously presented) The method of claim 1, wherein the identifying step uses an the enforced delivery of a Web page to be used in a distribution and subscription of new subscribers without prior knowledge of serial numbers associated with the new subscriber's interface equipment and without requiring the subscribers to utilize special software.

28.   (previously presented) The method of claim 27, further comprising the step of using the enforced delivery of a Web page to reduce a volume of telephone support

7

requests by an enforced pre-announcement of known, future system outages due to scheduled maintenance.

29.   (previously presented) The method of claim 27, further comprising the step of using the identifier for detection of "signature" forms of Internet packets that indicate a presence of undesirable content.

30.   (original) The method of claim 29, wherein the undesirable content is a virus.

31.   (previously presented) The method of claim 29, further including the step of transmitting a message identifying the undesirable content to a provider.

32.   (previously presented) The method of claim 29, further including the step of transmitting a bulletin message identifying the undesirable content to the subscriber.

33.   (original) The method of claim 31, further including the step of logging the undesirable content identifying message.

34.   (previously presented) The method of claim 28, wherein there is further included a manually accessed provider information Web site and the transmitting step includes enforcing a delivery of other subscriber-beneficial information that is currently displayed on the manually accessed provider information Web site.

8

35.   (previously presented) The method of claim 16, further including the step of logging successful transmission of bulletin messages to each subscriber.

36.   (original) The method of claim 16, further including the step of logging interactive responses that have been requested within the policy.

37.   (previously presented) The method of claim 16, further including the steps of detecting and logging a number of simultaneously requested Web connections, based on the transmission of the bulletin messages.

38.   (original) The method of claim 37, further including the step of flagging subscribers that are utilizing more than one simultaneous device per subscription.

39.   (previously presented) The method of claim 16, further including the step of transmitting explanations to be issued, in an enforced manner, to subscribers, after a service interruption, in such a manner as to alleviate customer dissatisfaction by illuminating and explaining a problem and future efforts that are to be taken to eliminate such problems.

40.   (cancelled)

41.   (cancelled)

42.   (cancelled)

9